



FREE REPORT

PROTECT YOUR NETWORK

"What every business owner must know about protecting and preserving their network."

Don't trust your company's critical data and operations to just anyone.

What Every Small Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems

If you depend on your computer network to run your business, this is one report you don't want to overlook.

This report outlines, in plain non-technical English, the common mistakes small business owners make with their computer network — mistakes that cost thousands in lost sales, productivity, and repair bills — and gives you a proven way to reduce or completely eliminate the expense and frustration of these oversights.

YOU'LL DISCOVER

- 01** The single most expensive mistake most small business owners make when it comes to protecting their company data.
- 02** The universal misconception business owners have about their computer networks, and how it can end up costing between \$9,000 and as much as \$60,000 in damages.
- 03** Six critical security measures every small business should have in place.
- 04** How to greatly reduce — or even completely eliminate — frustrating crashes, slow performance, and other annoying computer problems.
- 05** How to avoid expensive computer repair bills and get all the computer support you need for a low, fixed monthly rate.

From the desk of Don Swan, Founder & Managing Partner — Lithic LLC

Dear Colleague,

Have you ever lost an hour of work on your computer? Now imagine losing days or weeks — or losing your client database, your financial records, and every work file your company has ever produced.

Imagine what would happen if your network went down for days and you couldn't reach your e-mail or the information on your PC. How frustrating would that be? Or what if a major storm, flood, or fire destroyed your office and all of your files? If a virus wiped out your server, do you have a recovery plan you feel confident in?

How quickly do you think you could recover — if at all?

Many small business owners ignore or forget about securing their network from these catastrophes until disaster strikes. By then it's too late and the damage is done.

“But That Could Never Happen To Me”

And other lies business owners like to believe about their businesses

After working with over 200 small and mid-size businesses across central Mississippi, we found that 6 out of 10 will experience some type of major network or technology disaster — ending up costing them between \$9,000 and \$60,000 in repair and restoration costs on average.

That doesn't even include the lost productivity, lost sales, and damaged client goodwill when a company can't operate or fulfill its promises because of technical problems.

It may be difficult to determine the exact financial impact computer problems have on your business, but you can't deny that they have a negative effect. If your business has ever ground to a screeching halt because a server crashed, you already have some idea of the cost.

Most Computer Problems Are Hidden, And Strike Without Warning At The Most Inconvenient Times

Hardware failure, viruses, spyware, and other problems usually aren't detectable until they strike — bringing a server down, losing data, or causing some other catastrophe. Viruses and spyware are particularly sneaky because they are designed to hide themselves while they do their damage. Spyware can quietly transmit information about you and your company to an outsider without ever being visible to you.

Even if your network was recently audited by a consultant, viruses, spyware, and hackers attack constantly. That is why we monitor our clients' networks continuously — you never know when a new threat is going to strike.

Unfortunately, most computer consultants only offer "break-fix" services: when something breaks, they come in and fix it. That may seem like a reasonable setup, but it leaves you wide open to threats, problems, and disasters, because it is reactive rather than proactive.

Proactive maintenance is not an upgrade. It is the difference between a problem you never hear about and a problem that closes your doors for a week.

Take A Look At These Statistics

What downtime and data loss actually cost the businesses it happens to.

501 hrs

Average network downtime companies experience every year — costing an average of 3.6% of annual revenue. *Infonetics Research*

93%

Of companies that lost their data center for 10 days or more due to a disaster filed for bankruptcy within one year; 50% filed immediately. *National Archives & Records Administration*

20%

Of small to medium businesses will suffer a major disaster causing loss of critical data every five years. *Richmond House Group*

40%

Of small to medium businesses that manage their own network will have it accessed by a hacker this year — and more than half won't know they were attacked. *Gartner Group*

\$50K/hr

46% of surveyed companies said each hour of downtime would cost them up to \$50,000; 28% said \$51,000–\$250,000; 18% said up to \$1 million; 8% said more. *Cost of Downtime Survey*

\$900

Average amount cyber-criminals stole from each of 3 million Americans in the past year — not counting PCs rendered useless by spyware. *Gartner Group*

What These Failures Are REALLY Costing Your Business

Even if you don't factor in the soft costs of lost productivity, there is a hard cost to repairing and restoring your network. Most major repairs require four to eight hours to get a network running again, and most consultants can't get on site for 24 to 48 hours. That means your network could be down for one to two days.

Since the average computer consultant charges over \$100 per hour plus a trip fee — and a surcharge if it's an emergency — the average repair runs \$600 to \$1,000, before any hardware or software costs. Over a year that's \$1,800 to \$3,000, without counting lost sales and work hours. Those numbers multiply quickly with larger, more complex networks.

100% of these disasters and restoration costs could have been completely avoided, or greatly mitigated, easily and inexpensively — with a little planning and proactive maintenance.

Why Small Businesses Are Especially Vulnerable

With constant changes to technology and the daily development of new threats, it takes a highly-trained technician to maintain even a simple three- to five-person network. But the cost of hiring a full-time, experienced technician isn't feasible for most small business owners.

In an attempt to save money, most try to handle their own in-house IT support and designate whoever has the most technical expertise as the part-time IT manager. This never works out: that makeshift IT person has another full-time job to do, and usually isn't skilled enough to properly support an entire network anyway.

The result is a network that is ill-maintained and unstable. Backups, virus updates, and security patches don't get timely attention, giving a false sense of security.

It's only a matter of time before the network crashes. If you're lucky it costs you a little downtime; but there's always a chance you end up like one of these companies.

CASE ONE · \$20,000**Auto body shop shells out \$20,000 to clean up a virus**

A local auto body shop with multiple locations learned the importance of preventative maintenance the hard way. Without warning, a virus was downloaded to their server and began replicating and attaching itself to files. It corrupted their data, impaired their customer management system, and immediately brought down their Exchange server — no e-mail in or out.

Preventing the disaster would have cost 1/25th of the price (\$800 per month), and they would have had better performance and fewer problems along the way. Instead they spent \$20,000 to remove the virus and restore the network — and even then, that fee only got them running again; their systems still weren't optimized, secured, or updated as they should have been.

CASE TWO · \$40,000 & 9 DAYS DOWN**Two failed hard drives cost a health products company \$40,000**

The back office of a health products company had two hard drives fail at the same time, losing a large number of critical customer files. When they asked us to recover the data from their system backups, we found the backups weren't functioning properly. They appeared to be backing up everything; in fact they were worthless.

Recovering the data off the failed drives took a team of disaster recovery specialists nine days and \$15,000, plus another \$25,000 in services to stabilize the network. Proper monitoring would have shown that the drives were failing and the backups weren't working — preventing the crash, the downtime, and the \$40,000.

CASE THREE · \$9,000, THREE TIMES OVER**Property management company spends \$9,000 on a simple, inexpensive repair**

A 10-user property management company wasn't monitoring or maintaining their server. From overuse and lack of maintenance it began to degenerate and eventually shut down under the load, taking their entire network down for two full days and costing \$3,000 in support fees — far more once you factor in ten employees' lost productivity.

They chose not to implement a preventative maintenance program, so the same problem happened again two months later: another \$3,000 and two more days down. Six months after that it happened once more, bringing the total to \$9,000 in hard costs plus tens of thousands in productivity — for a problem that could have been detected and prevented.

Six Things You Must Do, At A Minimum, To Protect Your Company

It's impossible to plan for every potential computer problem, but a little proactive monitoring and maintenance will help you avoid or greatly reduce the impact of the vast majority of disasters you could experience.

Unfortunately, most small business owners are conducting no proactive monitoring or maintenance at all, which leaves them completely vulnerable to the disasters you just read about. There are three reasons why:

1. They don't understand the importance of regular maintenance.
2. Even if they did, they don't know what maintenance is required or how to do it.
3. They are already swamped with more immediate day-to-day fires. If the network is working today, it goes to the bottom of the pile — so no one is checking that the backups work, that virus protection is current, that critical patches are applied, or that the network is healthy overall.

There are over 37 critical checks and maintenance tasks that need to be performed daily, weekly, and monthly. Here are the six that matter most for protecting your company.

01

Back up your files every day

It amazes me how many businesses never back up their network. Imagine writing the most important piece of information you could ever write on a chalkboard, and I come along and erase it. How are you going to get it back? Unless you remembered it or made a copy, you can't. There are any number of things that could cause you to lose data files. If the information matters to you, make sure more than one copy exists.

02

Check your backups regularly to make sure they work

This is another big mistake I see. Many owners set up a backup system and then never verify it. It's not uncommon for a system to appear to be backing up when it isn't — dozens of things can go wrong and leave your backup corrupt and useless. It isn't enough to back up; you have to check on a regular basis that the data is actually recoverable. Remember the health products company that spent \$40,000 recovering data they thought they had backed up.

03

Keep an offsite copy of your backups

What happens if a fire or flood destroys your server and your backup drive? That is how hurricane Katrina devastated businesses that were later forced into bankruptcy. What happens if your office is robbed and they take everything? An offsite backup is simply a smart way to make sure you can get your business running again in a relatively short period of time.

04

Make sure virus protection is always on and up to date

You'd have to be living under a rock not to know how devastating a virus can be. With attacks arriving through spam, downloads, instant messages, web sites, and e-mails from friends and clients, you cannot afford to be without current virus protection. A virus can corrupt your files and bring down your network — and it can also hurt your reputation. If you or an employee unknowingly spreads a virus to a customer, or a virus hijacks your address book, you're going to make a lot of people very angry.

05

Set up a firewall

Small business owners tend to think that because they are "just a small business," no one would waste time hacking their network. Nothing could be further from the truth. I've run experiments connecting a single computer to the Internet with no firewall; within hours, over 13 gigabytes of space was taken over by malicious code and files I could not delete. There are thousands of unscrupulous people out there who think it's fun to disable your computer simply because they can.

They strike randomly, searching the Internet for open, unprotected ports. As soon as they find one they delete files or download huge files that can't be removed, shutting down your hard drive. They can also use your computer as a zombie to store pirated software or send spam, which will cause your ISP to shut you down. If the malicious programs can't be deleted, you'll have to re-format the entire drive — losing everything, unless you were backing up properly.

06

Apply critical security patches as they become available

Without up-to-date security patches and virus definitions, hackers can reach your computer through something as simple as a banner ad or an e-mail attachment. Not long ago Microsoft published a bulletin on three newly discovered vulnerabilities that could let an attacker take control of a computer by tricking a user into opening a maliciously crafted picture. An update was released at the same time — but without a process for applying critical updates promptly, you were completely exposed.

Here's the compelling part: most hackers don't discover these loopholes themselves. They learn about them when the vendor announces the vulnerability and issues an update. That announcement is their cue to analyze the update and craft an exploit for every computer that hasn't yet installed the patch.

The window between the update and the exploit keeps shrinking. When the "nimda" worm was discovered in the fall of 2001, Microsoft had released the protective patch 331 days earlier — and plenty of administrators still hadn't applied it. By the summer of 2003 there were only 25 days between the update that would have stopped the "blaster" worm and the detection of the worm itself. Clearly, someone needs to be paying close attention to your systems.

THE SHORT VERSION

Daily backups. Verified backups. An offsite copy. Current virus protection. A real firewall. Patches applied the week they ship. Miss one and the rest stop mattering.

ANNOUNCING

A simple, easy way to make sure these disasters don't happen to your business

If you're thinking "this all sounds great, but I don't have the time or the staff to handle all of this work" — we have the solution. Through our **Managed IT Services** program, Lithic takes over the day-to-day management and maintenance of your computer network entirely, freeing you from expensive, frustrating computer problems, downtime, and security threats. You get all the benefits of a highly-trained, full-time IT department at a fraction of the cost.

In most cases we can cut your IT support costs by 30% to 50% while improving the reliability and performance of your network and eliminating spyware, spam, and downtime.

The Benefits Are Obvious

- **You'll eliminate expensive repairs and recovery costs.** Our monitoring and maintenance saves you money by preventing expensive network disasters from happening in the first place. We guarantee it.
- **You'll avoid trip fees and get faster support.** Remote monitoring lets us access and repair most network problems from our offices — no waiting around for an engineer to show up.
- **Faster performance, fewer glitches, practically zero downtime.** Parts of your system degrade over time, causing slowdowns, hangs, and crashes. Preventative maintenance keeps your computers in tip-top shape for maximum speed and reliability.
- **All the benefits of an in-house IT department without the costs.** As a managed network client you have immediate access to a knowledgeable support staff for any problem or question.

- **Substantial discounts on services you already buy.** Most IT firms nickel and dime you over every little thing. Under this program you pay one flat, affordable rate for all the support you need — no hidden charges, caveats, or disclaimers.
- **No more fear of a big, unexpected repair bill.** You can budget for network support the same way you budget rent or insurance.
- **You'll safeguard your data.** The data on the disk is always more important than the hardware that houses it. If you rely on your systems for daily operations, it's time to get serious about protecting that irreplaceable information.
- **You'll gain incredible peace of mind.** As a business owner you have enough to worry about. We make sure everything pertaining to your network's security and reliability is handled, so you don't have to think about it.

FREE SECURITY AUDIT · NORMALLY \$250

How disaster-proof is YOUR network?

If you are not doing the six things outlined in this report, your network is an accident waiting to happen — and the costliest mistake you can make is to ignore that in the false hope it could never happen to you.

Because you read this report, I'd like to give you a free Network Security Audit — normally \$250 — as a way of introducing our **Managed IT Services** program. During the audit I will come on site and...

- ✓ Pinpoint any exposure to hackers, viruses, spyware, spam, data loss, power outages, downtime, and even employee sabotage.
- ✓ Review your system backups to make sure your data *can* be recovered in a disaster — you don't want to discover corrupt backups after the fact.
- ✓ Scan your network for hidden spyware and viruses planted to steal information, deliver spam, and track your online activity.
- ✓ Look for hidden problems that cause error messages, slow performance, and network crashes.
- ✓ Answer any questions about your network, and give you a second opinion on any projects you're considering.

There Are No Strings Attached, But You Have To Hurry

As you might have guessed, I can't extend this offer forever — time and staff limitations simply won't allow it. If you want to say goodbye to computer problems and stop worrying about the security of your data from hardware failures, viruses, hackers, and other threats, sign up now for your free Network Security Audit.

There is absolutely no obligation and no pressure to buy anything, or to ever use our services again. This is simply an easy way for us to demonstrate how we can help your business at no risk to you.

THREE WAYS TO CLAIM YOUR FREE AUDIT

1

Fill in and return the request form on the next page.

2

Call me direct at 601-487-4444.

3

E-mail info@lithicit.com with "Security Audit" in the subject line — include your company name, address, and phone so I can follow up.

Good networking,

Don Swan

Founder & Managing Partner, Lithic LLC
601-487-4444 · info@lithicit.com · lithicit.com
503 Avalon Way, Suite D, Brandon, MS 39047

P.S. This offer for a free Security Audit won't be around forever. As much as we'd love to give these away to everyone, staff and time limitations won't allow it — which is why you must respond by the date shown on the request form. You have my word that you will be under no pressure or obligation to buy anything, or to ever use our services again.



“Yes! I want to make sure my network and company’s data are safe from harm.”

Please sign me up for a free Security Audit so I can be sure I’m doing everything possible to secure my network. I understand I am under no obligation to do or buy anything by requesting this audit, and that these audits are made available on a first-come, first-served basis.

PLEASE COMPLETE AND RETURN

NAME

TITLE

COMPANY

ADDRESS

CITY / STATE / ZIP

PHONE

E-MAIL

NUMBER OF PCS / OPERATING SYSTEM

E-MAIL THIS FORM TO
info@lithicit.com

OR CALL ME DIRECT AT
601-487-4444

This form must be completed and returned to our offices by December 31.

Here's What Our Clients Say About Lithic

If customer service is essential to you, choose Lithic

"By far, the single biggest benefit is the quick response when we have an issue, and those issues are handled quickly. The accessibility of their team to get help when I need it is unlike any other IT company I have worked with in the past."

Kelly Riley — Mississippi Professional Educators

Lithic makes IT look easy

"Lithic has been incredibly responsive — it's like having them in the building with you. They have helped us navigate constant growth with a stable IT environment. I recommend Lithic to everyone I know that deals with their company's IT systems. You get fast resolutions to problems, a fair and upfront billing structure with no surprises, and real help when you are planning IT purchases of software and hardware."

Clay Foster — Southern Electric Corporation

Great customer service that's readily available

"The biggest benefits from using Lithic are the quick response time and easy accessibility. If customer service and communication are essential to you, use Lithic!"

Josh Young — Southern Healthcare Agency



Human I.T. for Mississippi businesses.

Managed IT services, help desk, data backup and recovery, and network security — delivered by a team that answers when you call.

CALL

601-487-4444

E-MAIL

info@lithicit.com

ONLINE

lithicit.com

VISIT

**503 Avalon Way, Suite D
Brandon, MS 39047**